ZEROFOX

Weekly Intelligence Brief

Classification: TLP:GREEN

August 9, 2025

ZEROFOX®

Weekly Intelligence Brief

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 6:00 AM (EDT) on August 7, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

| This Week's ZeroFox Intelligence Reports 2

Monthly Geopolitical Assessment August 2025 2

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 15 2

Zerofox Intelligence Brief - The Accidental Insider Threat 2

| Cyber and Dark Web Intelligence Key Findings 4

Chinese Threat Actors in Billion-Dollar Card Theft 4

FinCEN Issues Notice on the Use of CVC Kiosks for Scam Payments and Other Illicit Activity 5

New Malware Campaign Exploits Shortcut Files to Hijack Systems 5

| Exploit and Vulnerability Intelligence Key Findings 6

CVE-2025-5394 7

CVE-2025-54119 8

| Ransomware and Breach Intelligence Key Findings 10

Ransomware Watch: Top Actors, Industry Impact, and Key Updates 10

Notable Data Breaches in the Past Week 14

| Physical and Geopolitical Intelligence Key Findings 17

Physical Security Intelligence: Global 17

Physical Security Intelligence: United States 18

| Appendix A: Traffic Light Protocol for Information Dissemination 20

| Appendix B: ZeroFox Intelligence Probability Scale 21

This Week's ZeroFox Intelligence Reports

Monthly Geopolitical Assessment August 2025

Russia is likely to continue escalating its military operations in Ukraine beyond the U.S. deadline. Political pressure from Western states for Israel to end the Israel-Hamas war is unlikely to be successful unless the United States joins in; therefore, stasis in the conflict is likely. The non-tariff investment commitments from the likes of the European Union (EU), South Korea, and Japan reflect U.S. policy priorities to keep those states under the U.S. defense, technology, and energy umbrella at the direct expense of Russian energy and Chinese technology. The next EU budget will likely feature cuts to the agricultural sector and increased investment in the "competitiveness" of EU businesses to make them less dependent on foreign technology and defense products, which is reflected in the lopsided EU-U.S. trade agreement. There has been an uptick in the detention of foreigners—including U.S. nationals—in China. Political and security crises in Bolivia, Pakistan, Sudan, and Thailand will likely continue for many months.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 15

The Underground Economist is an intelligence-focused series that highlights dark web findings from our ZeroFox Dark Ops intelligence team.

Zerofox Intelligence Brief - The Accidental Insider Threat

Unintentional insider threats represent an often overlooked attack vector that threat actors regularly exploit to gain unauthorized access to sensitive data and networks. Although unintentional and lacking overtly malicious intent, these behaviors risk impacting a company's reputation, operational continuity, and long-term competitiveness. Insiders inadvertently expose sensitive organizational data by falling victim to manipulation or mishandling information through unintentional lapses in adherence to security protocols. The consequences of unintentional insider threats are often immediate and severe and include losses of private customer data, proprietary information, and sensitive internal communication.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Chinese Threat Actors in Billion-Dollar Card Theft

What we know:

- A major Chinese cybercrime syndicate operation compromised up to 115 million U.S. payment cards between July 2023 and October 2024.
- The group used smishing (SMS phishing), fake e-commerce sites, and phishing-as-a-service (PhaaS) platforms to steal card data, which was then tokenized for use in mobile wallets such as Apple Pay.
- By bypassing multi-factor authentication and avoiding fraud alerts through strategic card limits per device, the operation has caused billions in losses and presents a new, harder-to-detect threat to the financial sector.

Background:

- A key figure known as “Lao Wang” created a PhaaS platform via the Telegram channel “dy-tongbu”, which grew rapidly and evolved from basic smishing attacks to sophisticated fake e-commerce scams advertised on major platforms.
- The syndicate has expanded its operations to include selling devices pre-loaded with stolen cards and targeting brokerage accounts.

What is next:

- By monetizing stolen data across multiple channels, the syndicate likely secures its revenue streams while protecting the identities of its members—making it difficult to disrupt their operations through any single law enforcement action or targeted countermeasure.
- This method likely enables prolonged, large-scale theft without triggering alerts, leading to financial losses for banks and consumers and higher fraud-related costs for merchants.

FinCEN Issues Notice on the Use of CVC Kiosks for Scam Payments and Other Illicit Activity

What we know:

- The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has urged financial institutions to monitor and report illicit activity (including scams, cybercrimes, and drug trafficking) involving convertible virtual currency (CVC) kiosks.

Background:

- CVC kiosks—similar to ATMs but for buying and selling digital assets—are often placed in high-traffic locations. The risk of illicit activity is exacerbated if CVC kiosk operators fail to meet their obligations under the Bank Secrecy Act (BSA).

Analyst note:

- Illicit activity involving CVC kiosks includes fraud, certain types of cybercrime, and drug trafficking organization activity, with scams often targeting vulnerable populations and causing severe financial and emotional harm.

New Malware Campaign Exploits Shortcut Files to Hijack Systems

What we know:

- A deceptive malware campaign has been identified using malicious shortcut (.LNK) files on a popular desktop operating system to deliver the REMCOS remote access trojan.

Background:

- The campaign begins with a fake purchase order shortcut file. It uses Base64 encoding and a disguised .PIF file to install REMCOS while avoiding detection by security tools.

Analyst note:

- REMCOS provides attackers with full remote access, enabling keylogging, file theft, and surveillance through webcams and microphones that is likely to lead to credential theft, espionage, or lateral movement within corporate networks. If left unchecked, it could further fuel ransomware attacks, corporate sabotage, or large-scale data breaches.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog and released two Industrial Control Systems (ICS) advisories. Adobe has issued emergency patches for two zero-day vulnerabilities (CVE-2025-54253 and CVE-2025-54254) in Adobe Experience Manager (AEM) Forms on JEE, following the public release of a proof-of-concept exploit chain. Google has released Android security updates for August 2025 that address several vulnerabilities, including multiple actively exploited flaws in Qualcomm components. Researchers have uncovered a high-severity vulnerability (CVE-2025-54136) in the AI-powered code editor Cursor, which could lead to remote code execution. CVE-2025-54955 enables an unauthenticated attacker to exploit a timing issue and obtain a valid JSON Web Token (JWT) belonging to a legitimate user, all without needing their credentials. Trend Micro has disclosed two critical zero-day command injection vulnerabilities (CVE-2025-54948 and CVE-2025-54987) in the Apex One Management Console for Windows, one of which is actively exploited. A flaw in Broadcom BCM5820X chips used in over 100 Dell laptop models could enable attackers to steal sensitive data and retain access even after a fresh OS install. Researchers have discovered nine zero-day vulnerabilities in HashiCorp Vault and five in CyberArk Conjur, which are widely used password vaults relied on by thousands of organizations. Multiple vulnerabilities have been identified in the Python backend of NVIDIA's Triton Inference Server.

CRITICAL

CVE-2025-5394

What happened: Threat actors are exploiting this vulnerability in the "Alone – Charity Multipurpose Non-profit" WordPress theme (versions up to 7.8.3). The flaw, found in the alone_import_pack_install_plugin() function, lacks proper access controls, enabling unauthenticated users to upload and install arbitrary plugins. This enables full site takeover and remote code execution.

- **What this means:** Sites using vulnerable versions of the theme are at risk of compromise, potentially enabling attackers to deploy malware, steal data, or deface content. Users are advised to urgently update to version 7.8.5, which patches the vulnerability and prevents unauthorized access.

- **Affected products:**
    - Plugin versions prior to and including 7.8.3

CRITICAL

CVE-2025-54119

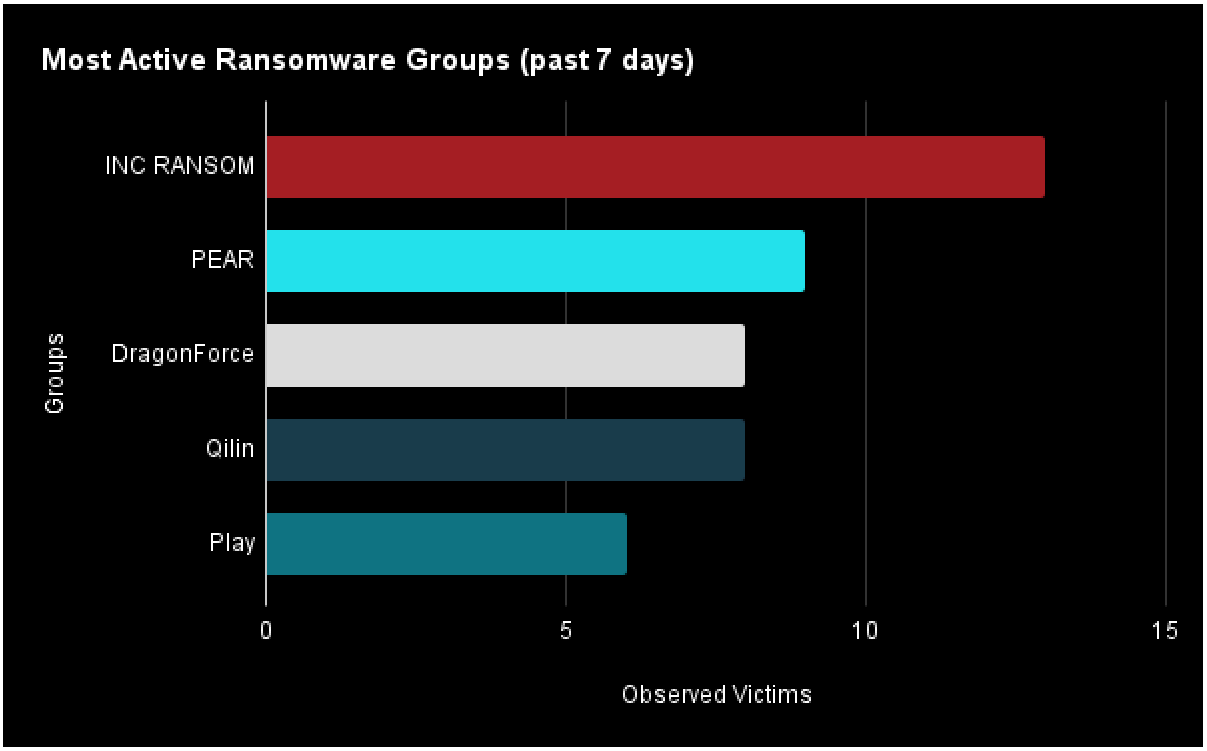
What happened: This vulnerability in ADOdb stems from improper escaping of query parameters when interacting with sqlite3 databases. If an attacker supplies a crafted table name to the metaColumns(), metaForeignKeys(), or metaIndexes() methods, they could execute arbitrary SQL commands.

- **What this means:** Applications using vulnerable ADOdb versions with untrusted input in these methods are at risk of SQL injection attacks. To mitigate the risk, developers are advised to update to version 5.22.10 or ensure only trusted data is passed to the affected methods' $table parameter.
- **Affected products:**
    - ADOdb versions 5.22.9 and below

Ransomware and Breach Intelligence

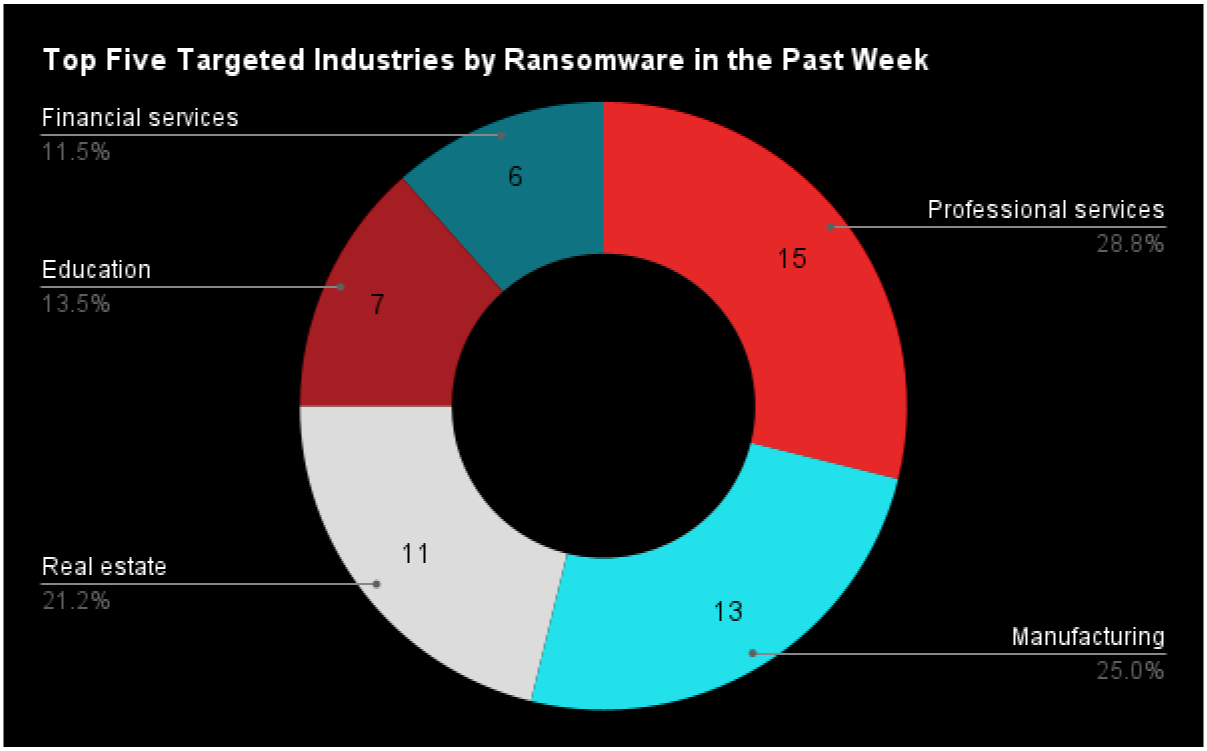
Ransomware and Breach Intelligence Key Findings

Ransomware Watch: Top Actors, Industry Impact, and Key Updates



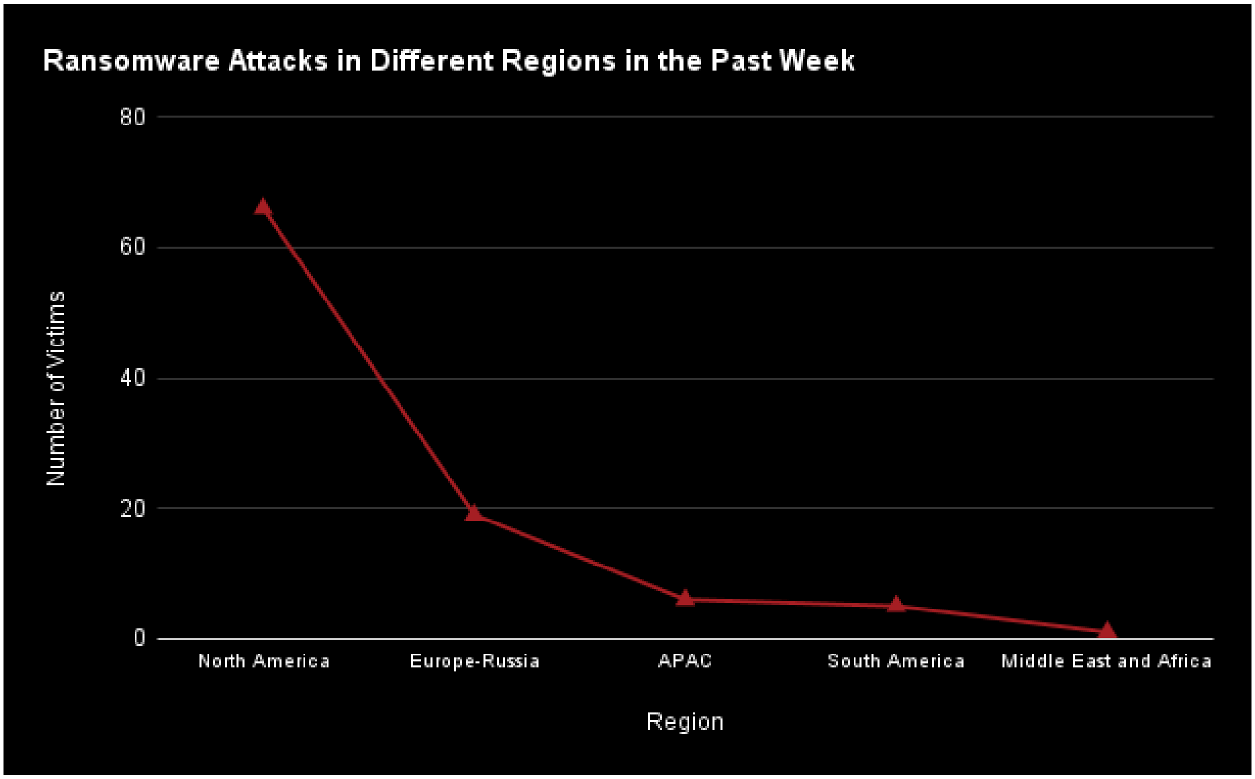
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, INC RANSOM, PEAR, DragonForce, Qilin, and Play were the most active ransomware groups. ZeroFox observed at least 96 ransomware victims disclosed, most of whom were located in North America. The INC RANSOM ransomware group accounted for the largest number of attacks, followed by PEAR.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that professional services was the industry most targeted by ransomware attacks, followed by manufacturing, real estate, education, and financial services.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe-Russia. There were 66 ransomware attacks in North America, while Europe-Russia accounted for 19, Asia-Pacific (APAC) for six, South America for five, and Middle East and Africa for one.

Recap of major ransomware events observed in the past week: Change Healthcare has confirmed that the number of individuals impacted by its February 2024 ransomware attack is slightly higher than initially estimated. The updated figure now stands at approximately 192.7 million, up from the previously reported 190 million. Storm-2603, a suspected China-based threat group, has exploited vulnerabilities CVE-2025-49706 and CVE-2025-49704 to deploy the Warlock ransomware strain, leveraging a custom command-and-control (C2) framework known as AK47 C2. The Akira ransomware group is suspected of exploiting a previously unknown zero-day vulnerability in SonicWall firewall devices, following a surge in cyberattacks targeting these devices since July 2025. ZeroFox has observed a new ransomware leak site named "PEAR" (Pure Extraction And Ransom). The Medusa ransomware group has claimed responsibility for a cyberattack on Highlands Oncology Group that has impacted 113,575 individuals, according to a recent disclosure to the Maine Attorney General.

Notable Data Breaches in the Past Week

Targeted Entity	**Columbia University**	**Pandora**	**Chanel**
Compromised Entities/Data Set	53 GB of student and alumni data	Not yet confirmed	Not yet confirmed
Compromised Data Fields	Bank account numbers, financial disbursements, test scores, grade-point averages, class schedules, home addresses, and other information	Customers' names, dates of birth, and email addresses	Names, email addresses, mailing addresses, and phone numbers
Suspected Threat Actor	Not yet determined	ShinyHunters	ShinyHunters
Country/Region	United States	United States	United States
Industry	Education	Retail	Retail
Possible Repercussions	Identity theft, fraud, and physical and online privacy violations	Impersonation, financial fraud, phishing, extortion, and data sale in dark web forums	Targeted phishing attacks, fake mails, delivery frauds, impersonation, supply chain attacks, and extortion

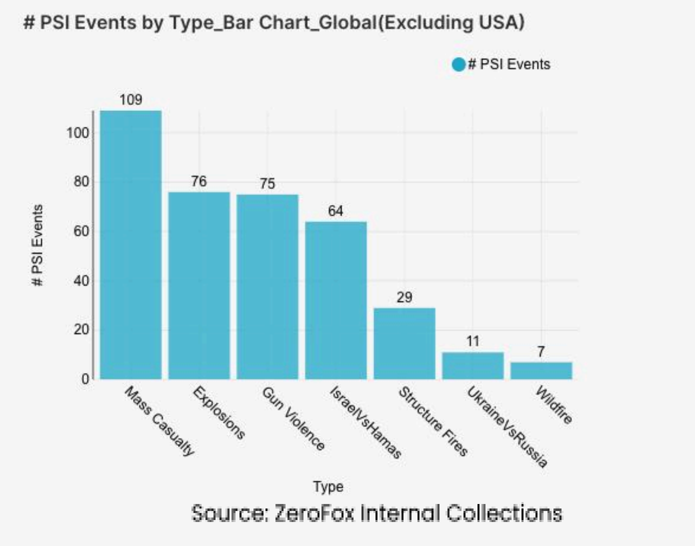
Three major breaches observed in the past week

Other major data breaches observed in the past week: KLM Royal Dutch Airlines suffered a data breach via a compromised third-party platform that has exposed personal information, including names, contact details, and loyalty program data. The threat actors have not breached core systems or exfiltrated more sensitive data. Cisco has confirmed a data breach that is likely a part of the ongoing Salesforce breach campaign, though the company has not confirmed any association at the time of writing. Pi-hole, a network-level ad-blocker, has disclosed a data breach affecting nearly 30,000 donors after a vulnerability in the GiveWP WordPress plugin exposed names and email addresses. The flaw made donor data publicly accessible in the website's source code, leading to reports of suspicious emails.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

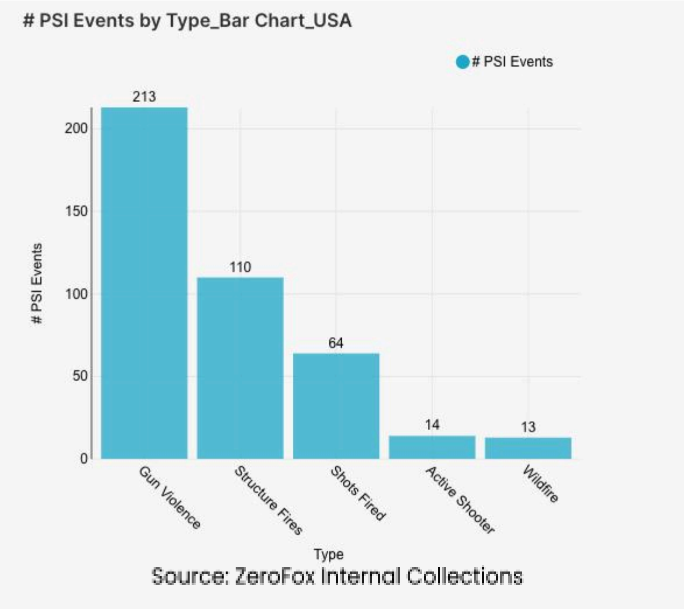


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 6 percent decrease in mass casualty events this week from the previous week, with the top contributing countries and territories being the Palestinian Territories, Syria, and Argentina, in that order. Approximately 70 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 32 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) decreased by 10 percent from the previous week. Events related to Russia's war in Ukraine increased by 38 percent. The top three most-alerted subtypes were explosions, which saw a 1 percent decrease from the previous week; gun violence, which increased by 25 percent; and structure fires, which increased by 26 percent. Global protest activity decreased by 26 percent.

- **What this means:** Despite a small decrease in overall mass casualty events, several regions experienced significant violence and crises this week. For instance, France's recent wildfire, which started on August 5, has burned an area larger than Paris, killing one and injuring over a dozen, including firefighters. This highlights increasing structure fire alerts and environmental impact on physical security. Events related to Russia's war in Ukraine saw a sharp increase in alerts as well, marked by a recent deadly missile and drone attack on Kyiv that killed 13 people and injured more than 130 on July 31. Russian President Vladimir Putin faces an August 8 deadline set by U.S. President Donald Trump to agree to a peace deal with Ukraine or face severe sanctions. In Syria, the conflict with the Druze minority has seen a resurgence, with recent clashes beginning on August 2 in the southern province of Sweida straining an already fragile ceasefire. These examples reveal that physical security threats are becoming increasingly diverse and interconnected, with traditional conflicts, environmental crises, and civil unrest all contributing to a dynamic and unpredictable risk landscape.

Physical Security Intelligence: United States

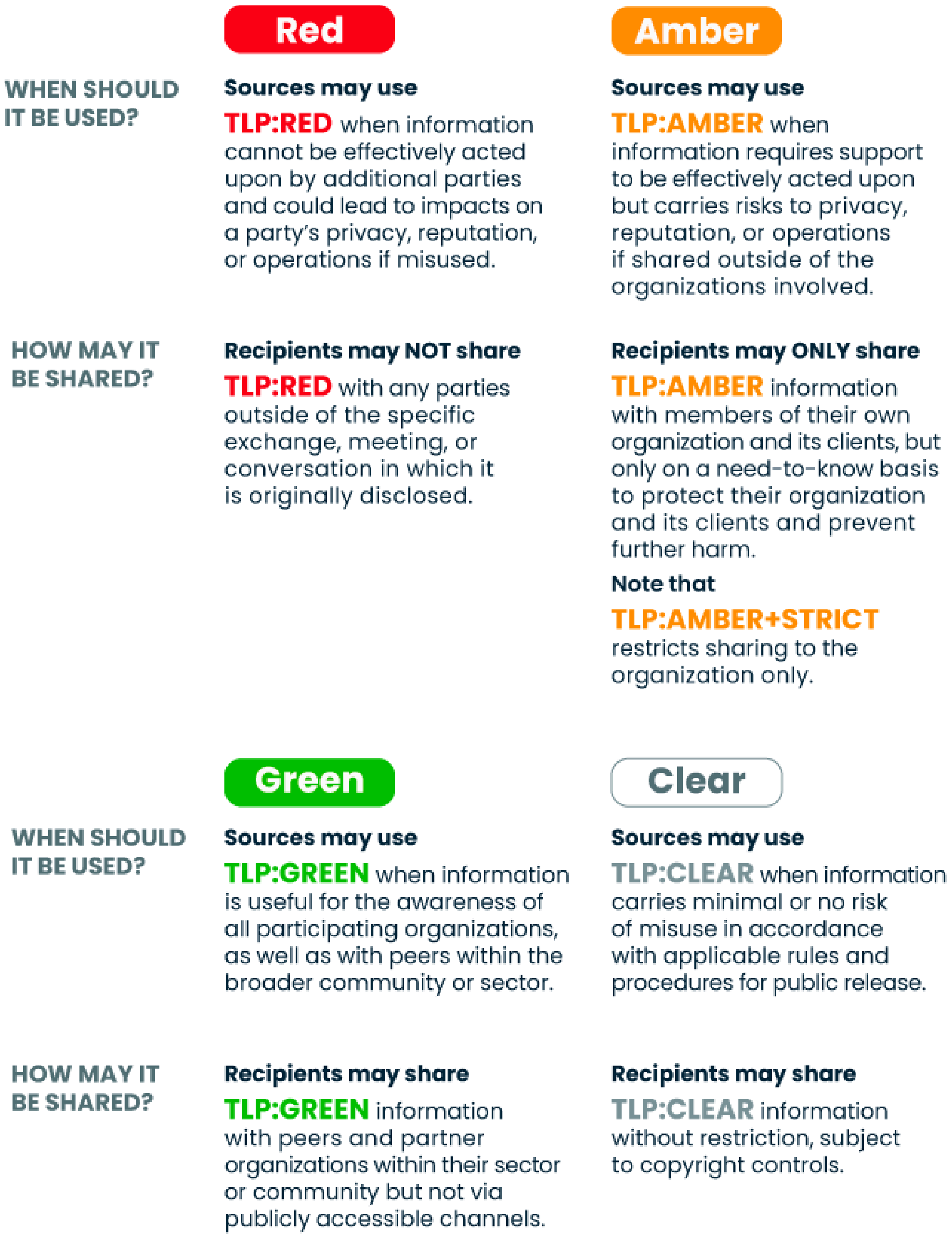


Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, structure fires are fires that affect man-made buildings, and shots fired are shootings with no confirmed victim. The top two states that had the most gun violence alerts were Illinois and Ohio, which together made up 22 percent of this week's nationwide total. Gun violence across the United States overall decreased by 20 percent from the previous week. Shots fired alerts increased by 7 percent, and the top contributing states were also Illinois and Ohio. Structure fires decreased by 13 percent, and the top two states for this subtype were California and New York. Additionally, wildfire alerts increased by 63 percent nationwide. Notably, active shooter alerts increased by 27 percent.

- **What this means:** In the past week, the United States saw a complex and shifting landscape of physical security threats. While gun violence decreased nationwide, specific regions remained hotbeds for these incidents, with Illinois and Ohio together accounting for over one-fifth of all gun violence and shots fired alerts. One notable trend was the sharp increase in active shooter alerts; for instance, on August 6, a sergeant shot and injured five soldiers at Fort Stewart in Georgia, prompting a swift lockdown and a major law enforcement response. Simultaneously, the country grappled with a significant rise in environmental and man-made disasters. Although structure fires affecting buildings decreased overall, wildfire alerts nationwide surged. California remains a top state for both types of fires, with a large wildfire currently moving through Los Padres National Forest and having already burned over 129 square miles, threatening hundreds of structures. These events highlight the diverse and evolving nature of physical security threats, which include deliberate attacks, as well as natural and man-made disasters.

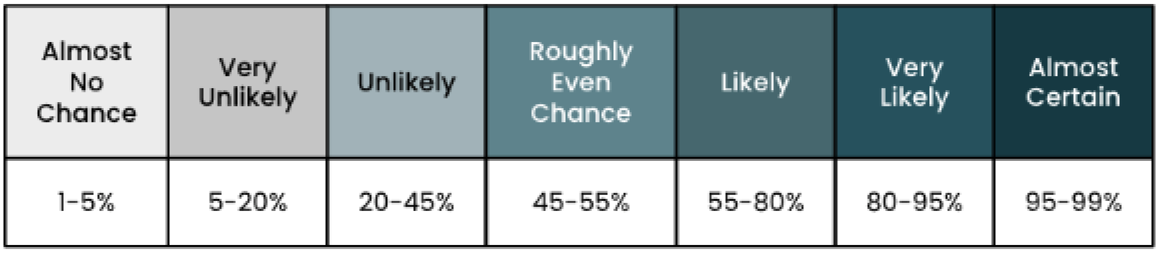
Appendix A: Traffic Light Protocol for Information Dissemination



	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	**Clear**
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%